UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 1101 3rd Street Southwest, Apartment 304, Washington, DC 20024	)	Case No. 11-037-M-01

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the ________ District of Columbia
(identify the person or describe the property to be searched and give its location):
1101 3rd Street Southwest, Apartment 304, Washington, DC 20024, as further described in ATTACHMENT A, which is attached hereto and incorporated fully herein.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
evidence of violations of 18 U.S.C. Section 1030(a)(5), as further described in the attached affidavit in support of search warrant incorporated fully herein (including ATTACHMENT B)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before February 9, 2011
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. □ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

____________________ .
(name)

□ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* □for ____ days *(not to exceed 30)*
□until, the facts justifying, the later specific date of ________ .

Date and time issued: JAN 26 2011 @ 1:13 pm

Judge's signature

City and state: Washington, D.C.

DEBORAH A. ROBINSON, U.S. MAGISTRATE JUDGE
Printed name and title

Return

Case No.: 11-037-M-01	Date and time warrant executed: 01/27/2011 2:10 pm	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

See Attached

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 01/28/2011

Amy Renee Liggett
Executing officer's signature

SA Amy Renee Liggett
Printed name and title

U.S. DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

On (date) [illegible]/27/2011

At (time) 5:40 PM

(Name) ___

(Location) 1101 3rd Street SW, Apt. #304
Washington, DC 20024

Item(s) listed below were:
□ Received From
□ Returned To
□ Released To
☒ Seized

ITEM#	DESCRIPTION
1	Apple iPod 30 GB, Black, seial #8R6473NFV9M
2	Notebook
3	Sony PCG 612IL SN# 3101601 & power supply
4	ComCast billing statement dated 12/14/2010
5	Kingston 16 GB thumb drive containing memory capture of Sony Laptop
6	WD USB hard drive with power supply
7	Five pages of Future Dial, Inc. phone contacts dated 8/20/04
8	3 prescription pads
9	Micro Center 8 GB USB drive
10	Kingston 8GB Flash w/ RAM dump

(END OF LIST) Total of 10 Item(s) Listed

This is to certify that Special Agents of the Federal Bureau of Investigation, U.S. Department of Justice, at the time of conducting a search of my person and/or the property (1101 3rd Street SW, Apt. #304 Washington, DC 20024) obtained the above listed items. I further certify that the above represents all that was obtained by Special Agents of the Federal Bureau of Investigation, U.S. Department of Justice.

Witnesses:

Special Agent
Federal Bureau of Investigation
U.S. Department of Justice

Special Agent
Federal Bureau of Investigation
U.S. Department of Justice

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 1101 3rd Street Southwest, Apartment 304, Washington, DC 20024	)	Case No. 11-037-M-01

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
1101 3rd Street Southwest, Apartment 304, Washington, DC 20024 (as further described in the attached affidavit in support of search warrant incorporated fully herein, including ATTACHMENT A)

located in the District of Columbia, there is now concealed *(identify the person or describe the property to be seized)*:
evidence of violations of 18 U.S.C. Section 1030(a)(5), as further described in the attached affidavit in support of search warrant incorporated fully herein (including ATTACHMENT B).

The basis for the search under Fed. R. Crim P. 41(c) is *(check one or more)*:

☑ evidence of a crime;

□ contraband, fruits of crime, or other items illegally possessed;

□ property designed for use, intended for use, or used in committing a crime;

□ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 U.S.C. Section 1030(a)(5)	Knowingly Causing the Transmission of a Program, Information, Code or Command and Intentionally Causing Damage to a Protected Computer

The application is based on these facts:

SEE ATTACHED AFFIDAVIT HEREIN INCORPORATED BY REFERENCE AS IF FULLY RESTATED HEREIN

☑ Continued on the attached sheet

□ Delayed notice of ___ days (give exact ending date if more than 30 days: ______) is requested under 18 U.S.C § 3103a, the basis of which is set forth on the attached sheet.

Amy Renee Liggett
Applicant's signature

Amy Renee Liggett, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: JAN 26 2011

Deborah A. Robinson
Judge's signature

City and state: Washington, D.C.

DEBORAH A. ROBINSON, U.S. MAGISTRATE JUDGE
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE)
SEARCH OF THE PREMISES')
KNOWN AS 1101 3RD STREET SW,)
APARTMENT 304,) Magistrate No. 11-037-M-01
WASHINGTON, DC 20024)
)
)

AFFIDAVIT AND APPLICATION FOR SEARCH WARRANT

I, Amy Renee Liggett, being duly sworn, do hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe there exists evidence, fruits, and instrumentalities of violations of criminal laws, namely, Title 18, United States Code, Section 1030(a)(5) (Knowingly Causing the Transmission Of A Program, Information, Code Or Command and Intentionally Causing Damage To A Protected Computer), and conspiracy to commit that offense, at the residence located at 1101 3RD STREET SW, APARTMENT 304, WASHINGTON, DC 20024 (hereafter the "SUBJECT PREMISES"), more fully described in Attachment A. Accordingly, I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the SUBJECT PREMISES for certain things particularly described in Attachment B.

2. I am a Special Agent ("SA") with the FBI assigned to the Washington Field Office Criminal Division, and have been so employed since July 2010. My training included attending the twenty-week FBI New Agent Basic Training, during which I received instruction on various aspects of federal investigations. In addition to new agent training, I have assisted in numerous investigations to include search warrant executions regarding cyber related criminal

activity. I have conducted and observed interviews of individuals believed to be involved in cyber crimes for the purpose of securing information pertaining to cyber criminal violations.

3. I am familiar with the facts and circumstances of this case. The facts set forth in this affidavit are based on knowledge obtained from other FBI agents and other individuals; my review of documents and computer records related to this investigation; oral and written communications with others who have personal knowledge of the events and circumstances described herein; review and analysis of computer information obtained from the victim organizations; review of public source information, including information available on the Internet; and records received via legal process. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

THE SUBJECT PREMISES

4. The SUBJECT PREMISES is located at 1101 3RD STREET SW, APARTMENT 304, WASHINGTON, DC 20024. The SUBJECT PREMISES is located on the instersection of M Street SW and 3rd Street SW. The SUBJECT PREMISES is a high-rise, multi-family apartment building, also known as the Waterfront Tower building. The number 1101 is located on the right pillar directly in front of the main entrance into the Waterfront Tower building. The Waterfront Tower is a gated community with electronic keypad access into the parking lot, the main building entrance, and into the exterior stairwells and interior elevators. The entrance into the building parking lot is located off of M Street near the intersection of M Street and 3rd Street. Apartment 304 is an interior unit and is located on the west side of the third floor of the main entrance building. Apartment 304 has a brown door with the numbers "304" located to the right

side of the door.

APPLICABLE STATUTES

5. Title 18, United States Code, Section 1030(a)(5) states:

> (a) Whoever - (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished as provided in subsection (c) of this subsection.

DEFINITIONS

6. The following terms, with which I am familiar as a result of my training, education, and experience, are pertinent to this investigation:

7. Domain Names: Numerical IP addresses may have corresponding domain names. For instance, the IP address "149.101.10.40" resolves to the corresponding domain name "*www.cybercrime.gov.*"

8. Internet Protocol Address: An Internet Protocol ("IP") address is a unique numeric address used to identify computers on the Internet. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. IP addresses are typically assigned by Internet service providers ("ISPs"), such as AOL, Earthlink. or AT&T, or Comcast. An ISP might assign a different IP address to a customer each time the customer makes an Internet connection (so-called dynamic IP addressing). or it might assign an IP address to a customer permanently or for a fixed period of time (so-called static IP addressing). In both scenarios. the IP Address used by a computer attached to the Internet must be unique. ISPs typically log their customers' connections. which means the ISP can identify which of their customers was assigned a specific

IP address during a particular session.

9. User Datagram Protocol ("UDP"): A basic Internet protocol with which computer applications can send messages to other computers on the Internet without requiring prior communications to set up special transmission channels or data paths.

10. Transmission Control Protocol ("TCP"): A basic Internet protocol that provides the service of exchanging data between two hosts. TCP provides reliable ordered delivery of a stream of data from a program on one computer to another program on another computer.

11. Hypertext Transfer Protocol ("HTTP"): A networking protocol for distributed, collaborative, hypermedia information systems. HTTP is a communication protocol that is the foundation of data communication for the World Wide Web.

12. Log files: The term "log files" refers to computer-generated files containing information regarding the activities of computer users, processes running on a computer, and the activity of computer resources.

13. Internet Relay Chat ("IRC"): is a form of real-time Internet chat. It is mainly designed for group (many to many) communication in discussion forums called channels, but also allows one to one communication via private message. An IRC server can connect to other IRC servers to expand the network. Users access IRC networks by connecting to a client server. Most client servers do not require users to register an account but a user will have to set a nickname before being connected.

14. Distributed Denial of Service ("DDoS") Attack: is an attack which is an attempt to make a computer resource unavailable to it intended users. Although the means to carry out. motives for. and targets of a DDoS may vary. it generally consists of the concerted efforts of a person or people to prevent an internet site or service from functioning efficiently or at all. One

common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds slowly as to be rendered effectively unavailable.

15. LOIC/HOIC: Low Orbit Ion Cannon/High Orbit Ion Cannon are packet-flooding tools using UDP, TCP, and HTTP methods. LOIC and HOIC are open source computer programs that were designed as network stress testing applications. LOIC was initially written as a network stress-testing application, requiring the user to enter details on the types of requests they wished to send and the target host. LOIC was subsequently modified to installations of the software to be directed remotely, which the attackers frequently refer to as a "hive" or "hive mind." Attackers can use this tool to send extremely large amounts of packets over the network to attempt to overwhelm a target. LOIC may be used collectively by numerous sources to conduct a DDoS attack, flooding the target site with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of the target site. LOIC may be used in two ways, manual or HIVE Mode (also known as "HIVE Mind"). If using manual mode, the LOIC user must enter a target, such as an IP address or the http address of the target.

16. Strings: A string is a sequence of characters, generally understood as a data type storing a sequence of data values. As explained below, copies of the LOIC applications involved in this investigation used a limited set of strings containing specific unique data values, creating identifiable signatures..

17. HIVE and/or HIVE Mind: This mode of LOIC enables the user to target their copy of the application to an IRC server. allowing someone else to control the target at which connected LOIC clients are aimed. The user is basically agreeing to participate in a "voluntary" botnet.

18. Botnet: is a jargon term for a collection of software robots, or bots, which run autonomously. This can also refer to the network of computers using distributed computing software. While the term "botnet" can be used to refer to any group of bots, such as IRC, the word is generally used to refer to a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common "command and control" infrastructure. A botnet's originator, referred to as a "botherder," can control the group remotely through communications using a specific protocol, usually IRC, and usually for nefarious purposes.

19. Twitter: is an Internet service owned and operated by Twitter, Inc., which offers social networking and micoblogging services, enabling its users to send and read short messages called "tweets." Tweets are text based posts displayed on a user's profile page. Twitter users may subscribe, or "follow," other users' tweets. Tweets are publicly visible by default; however, senders can restrict message delivery to their followers.

20. Radware: is an intrusion prevention system or a network utility device that can be connected to a company's network and is designed to provide security and detect known intrusion attacks. It is designed to examine all network traffic and determine which traffic to allow into the network.

FACTS SUPPORTING PROBABLE CAUSE

Executive Summarv

21. As explained in more detail below, this investigation involves Distributed Denial of Service ("DDoS") attacks against PayPal, Inc. ("PayPal"), a wholly-owned subsidiary of eBay, Inc., in San Jose, California. The scheme, known as "Operation Payback," was organized by an online group known collectively as "Anonymous" in response to PayPal's publicized

decision to suspend the PayPal account of the WikiLeaks organization, which had been used by WikiLeaks to collect donations. At the direction of members of Anonymous, disseminated primarily via the online messaging service Twitter, volunteers downloaded specialized "LOIC" software to their computers which allowed them to participate in the DDoS attacks against PayPal. Once installed, the LOIC software was either manually targeted at PayPal by the user or was configured by the user to retrieve targeting information remotely from a computer server (the "HIVE Mind"). PayPal employed a network protection device which logged data regarding the DDoS attacks and, in some cases, associated traffic from particular IP addresses with the LOIC software and the configuration strings known to be associated with Operation Payback. PayPal disclosed logs to the FBI, which indicated that a particular IP address, 68.48.89.210, was responsible for sending DDoS traffic to PayPal on December 9th and 10th, 2010. Records subsequently received from Comcast show that the IP address 68.48.89.210 was assigned to a subscriber at the SUBJECT PREMISES on December 9th. In my training and experience, these facts establish probable cause that a person at the SUBJECT PREMISES downloaded the LOIC software and used it to participate in Operation Payback.

<u>Overview of DDos Attacks Against PayPal ("Operation Payback")</u>

22. On December 6. 2010. PayPal FBI Supervisory Special Agent ("SSA") William Ng, SA Melanie Adams, and SA Christopher Calderon participated in a conference telephone call with

PayPal. During the conversation and subsequent contacts, indicated that PayPal had posted a message about suspending the WikiLeaks' PayPal account on its blog site. *www.paypalblog.com*: further advised that on December 4, 2010, PayPal's blog had experienced a minor DDoS attack. believed that an Internet activist group that uses the names "4chan" and "Anonymous" (hereinafter referred to collectively as "Anonymous") appeared to be organizing a larger DDoS attack against PayPal. believed the attack was organized in response to PayPal's decision to suspend WikiLeaks'[1] PayPal account that was used by the operators of WikiLeaks to collect donations.[2] According to a press release issued by Anonymous and cited by several Internet news articles and magazine reports, Anonymous, describe themselves as being "average Internet Citizens" and state that their "motivation is a collective sense of being fed up with all the minor and major injustices we witness every day."

23. Later in the morning, on December 6, 2010, advised the FBI that there had been a DDoS attack against PayPal's website. On December 10, 2010, PayPal, advised SA Melanie Adams there had been multiple, severe DDoS attacks against eBay/PayPal between December 6, 2010 and December 10, 2010, which were coordinated by a group referred to as both "Anonymous" and "AnonOps." also advised the FBI that on December 8, 2010, the website *www.paypal.com* was attacked with a large scale, coordinated DDoS effort directed by IRC servers controlled by Anonymous. This attack peaked around 7 pm PST. further advised that on December 10, 2010, PayPal was still experiencing unusual traffic levels

[1] WikiLeaks is an international organization that publishes submissions of otherwise unavailable documents from anonymous sources. The WikiLeaks website states that they provide an innovative, secure and anonymous way for independent sources around the world to leak information. WikiLeaks recently released a large amount of classified United States State Department cables to the public in late November 2010. In response to WikiLeaks' release of the classified cables, many companies that conducted business with WikiLeaks, such as PayPal, Visa, Amazon, and Mastercard suspended or froze WikiLeaks' accounts, citing a violation of their terms of service. Many of the companies that terminated their relationship with WikiLeaks are now being targeted by online activist groups such as Anonymous.

[2] PayPal indicated that it posted the message about suspending the WikiLeaks account on December 3, 2010, on its blog site (www.thepaypalblog.com). On December 4, 2010, PayPal's blog experienced a minor DDoS attack believed to be initiated by Anonymous. Additional chatter was heard on the Internet suggesting that Anonymous would launch more serious attacks against PayPal.

including low levels of attack traffic.

24. According to news reports and national and international law enforcement reports, in addition to PayPal, the attackers have launched DDoS attacks against numerous other online entities including Visa, Mastercard, Moneybookers.com, Sarah Palin's website, and the Swedish Prosecutor's Office. Anonymous has titled their attacks "Operation Payback."

25. On or about December 13, 2010, SA Christopher Calderon reviewed a number of Twitter feeds relating to Operation Payback. Based on the review of Twitter feeds, it appeared that the attackers, whose identities were obscured by nicknames, were not concealing their actions, but actually trying to make the attacks highly publicized. The attackers were primarily organizing and recruiting participants through Twitter, using Twitter accounts such as "Anon_Operation," "AnonOpsNet," "Operation_Anon," "Anon_Operations," and "Op_Payback." Ultimately, Anonymous recruited participants and then directed those who wanted to participate in the attack to their IRC server at *irc.anonops.net* (the anonops IRC server). For instance, publicly viewable posts were being made on various Internet sites including Twitter which read:

> "Target: https://www.paypal.com/ When: in a few hours. We will fire at anyone or anything that tries to censor WikiLeaks, including multi-Billion dollar companies such as PayPal. Twitter you're next for censoring #wikileaks discussion. Set you local HIVE server to loic.anonops.net, channel #loic. Get on our IRC network! irc://irc.anonops.net/Operation Payback http://www.anonops.net."

26. Based on the review of these Twitter feeds by SA Calderon on or about December 13, 2010, it appeared that once users logged into the anonops IRC server, they were instructed to download and install the LOIC computer program.

Use of the LOIC Application in the DDoS Attacks

27. A copy of the source code for the LOIC client used by Anonymous in Project Payback was obtained by eBay. analyzed the code to determine the way the LOIC client program functions and subsequently provided a detailed report to SA Adam Reynolds of the FBI.The copy was launched in an isolated test environment to determine the steps necessary to launch an actual attack, though the test copy was never allowed to connect to any other systems. This analysis was on just one available version of the LOIC client; other versions of LOIC were also used as part of Project Payback. Throughout the attack timespan, the LOIC application was being modified by its creators and contributors in order to improve its effectiveness. It is not believed, however, that any of those modifications resulted in material differences in LOIC's functionality; the attack patterns remained largely unchanged, with only minor differences in packet payload.

28. The LOIC application was designed to run on a Windows-based operating system (e.g., Windows XP, Windows Vista, Windows 7, etc). It was written in the C Sharp programming language, more commonly referred to simply as C#. C# is a language written and published by Microsoft Corporation, and is commonly available to software developers. C# is an internationally-known computer language used to create custom applications for Windows based-systems, the most widely installed personal computer operating system in the world.

29. A web-based LOIC tool also exists, but offers no automatic remote control capability. Unlike the Windows version, the web-based LOIC does not require the user to install an application, and is usable in any JavaScript-compatible web browser. This enables users on non-Windows systems (Mac. Linux. etc) to launch attacks. The web-based LOIC has been seen with default settings pointed to *https.//www paypal com.* however it still requires a user to

consciously launch the attack.

30. Neither mode can be initiated and, nor an attack launched, by merely launching either the Windows or web-based LOIC application. Both versions require some level of interaction from the user, whether to enter target details manually or to direct the application to a remote control server to choose targets.

31. According to Internet and open source records, within the anonops IRC server site there were a number of different channels administered by members of Anonymous. The different channels include "#loic-forks," "#operationpayback," "#propaganda," "#Setup," "#Status," and "#Target" among others. Within these channels, users discussed their opinions on Operation Payback, obtained technical support on how to install and use the LOIC program, and voted for which websites should be the next target of a DDoS attack.

32. According to Internet and open source records, in addition to the Twitter accounts described above, Anonymous uses the websites *www.anonops.net* and *www.anonops.com* to communicate between members and coordinate DDoS attacks. Anonymous members used *www.anonops.net* to coordinate the attack on PayPal as well as other victim entities.

PayPal Logs

33. On December 15, 2010, PayPal provided the FBI with logs and reports detailing approximately 1,000 IP addresses that sent malicious network packets to PayPal during the DDoS attacks. The 1,000 IP addresses were derived from logs created by a Paypal-owned Radware device. This list represents the IP addresses that sent the largest number of packets. Radware is a network utility device that was connected to PayPal's network and designed to provide security and detect intrusions or attacks. The Radware device is designed to examine all incoming network traffic and determine which traffic to allow in to the company's internal

network. Legitimate traffic is allowed to enter the internal network and traffic that appears to be malicious is blocked. The device works by recognizing specific signatures of known network attacks. If a malicious attack is recognized, the device first blocks the traffic and then creates a record in a log file detailing the attacker's IP address and the malicious signature recognized. The Radware device is designed to place priority on blocking the malicious attack instead of creating the record in the log file. Therefore, if the PayPal network was heavily attacked, the device might not log the malicious attack and instead, focus its resources on blocking the attack. Also, according to PayPal network engineers, the Radware device rarely recognizes legitimate network traffic as malicious traffic. This means it would be highly unlikely that the Radware device would confuse someone who is trying to use PayPal services legitimately with someone who is attacking PayPal. Further, in this particular instance, due to the specific known signatures used by the LOIC tool, there is a greater degree of certainty that the Radware device accurately identified the malicious traffic.

34. All of the attacks observed by eBay and PayPal engineers used a specific set of strings; only a half dozen variants were observed. and these were largely consistent across the source IP addresses observed for a given timespan of the attack period. This pattern suggests that attackers were either actively allowing their LOIC clients to be remotely-controlled with universally-applied parameters, or were intentionally placing these configuration details into their respective copies of the LOIC application when directed to do so.

35. Multiple string patterns were observed attacking PayPal systems simultaneously at various points throughout the attack period. This indicates that either multiple "hive mind" controls were in use. or that LOIC users were not following consistent instructions: however all patterns still fell within the same list of variants. The use of so few attack strings also suggests a

clear intent to attack PayPal systems, since those strings could not be obtained without knowing the purpose behind them.

36. The LOIC tools used to execute this attack contained the following specific PayPal-known signatures: wikileaks, wikileakshttp, goof, goofhttp, block-https-ascii, and goodnight.

<u>An IP Address Captured by PayPal is Linked to the SUBJECT PREMISES</u>

37. According to the logs provided by PayPal, between December 9, 2010, at 19:35 PST and December 10, 2010, at 13:45 PST, a computer assigned the IP address 68.48.89.210 sent approximately 114,238 packets to attack PayPal, containing the LOIC signature "goof."

38. On December 29, 2010, a Federal Grand Jury Subpoena was served on Comcast Corporation ("Comcast") requesting subscriber information for the subscriber assigned the IP address 68.48.89.210 on December 9, 2010, at 19:35:22 PST.

39. On January 07, 2011, a response was received from Comcast. The response revealed that the subscriber of the IP address was with a service address at the SUBJECT PREMISES.

40. On January 20, 2010, FBI SA Emily A. Odom conducted a search via CLEAR, a subscription based public and proprietary records database that can be accessed and searched over the Internet, for the SUBJECT PREMISES,. The search revealed possible residents at the address as and James C. Murphy, approximately 36 years of age.

41. Based on my training and experience. and knowledge of the LOIC application's functionality. I believe that the LOIC attack signatures observed during the DDoS attacks were a result of intentional and willful abuse, and not as a result of accidentally running the program

without understanding what was happening. The forensic data collected also establishes a clear pattern of attack traffic over time, showing in many cases a prolonged intent to cause damage to PayPal systems.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

42. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

44. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books. "chat." instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used. the purpose of their use. who used them. and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to attack a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience. I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

45. Searching storage media for the evidence described in the attachments may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above. because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence. including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant. a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally. it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

46. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant.

47. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

48. Based upon the information above, I have probable cause to believe that evidence, contraband, fruits, and/or instrumentalities of violations of Title 18, United States Code Section 1030(a)(5)(A)(Knowing Causing the Transmission Of A Program, Information, Code Or Command and Intentionally Causing Damage To A Protected Computer) exists at the SUBJECT PREMISES. Accordingly, I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

49. It is respectfully requested that this Court issue an order sealing. until further order of the Court. all papers submitted in support of this application. including the application

and search warrant. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Disclosure of the search warrant at this time would seriously jeopardize the investigation; such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Amy Renee Liggett

Amy Renee Liggett, Special Agent
Federal Bureau of Investigation

JAN 26 2011

Sworn to before me this ______
day of January, 2011

HONORABLE DEBORAH A. ROBINSON
UNITED STATES MAGISTRATE JUDGE

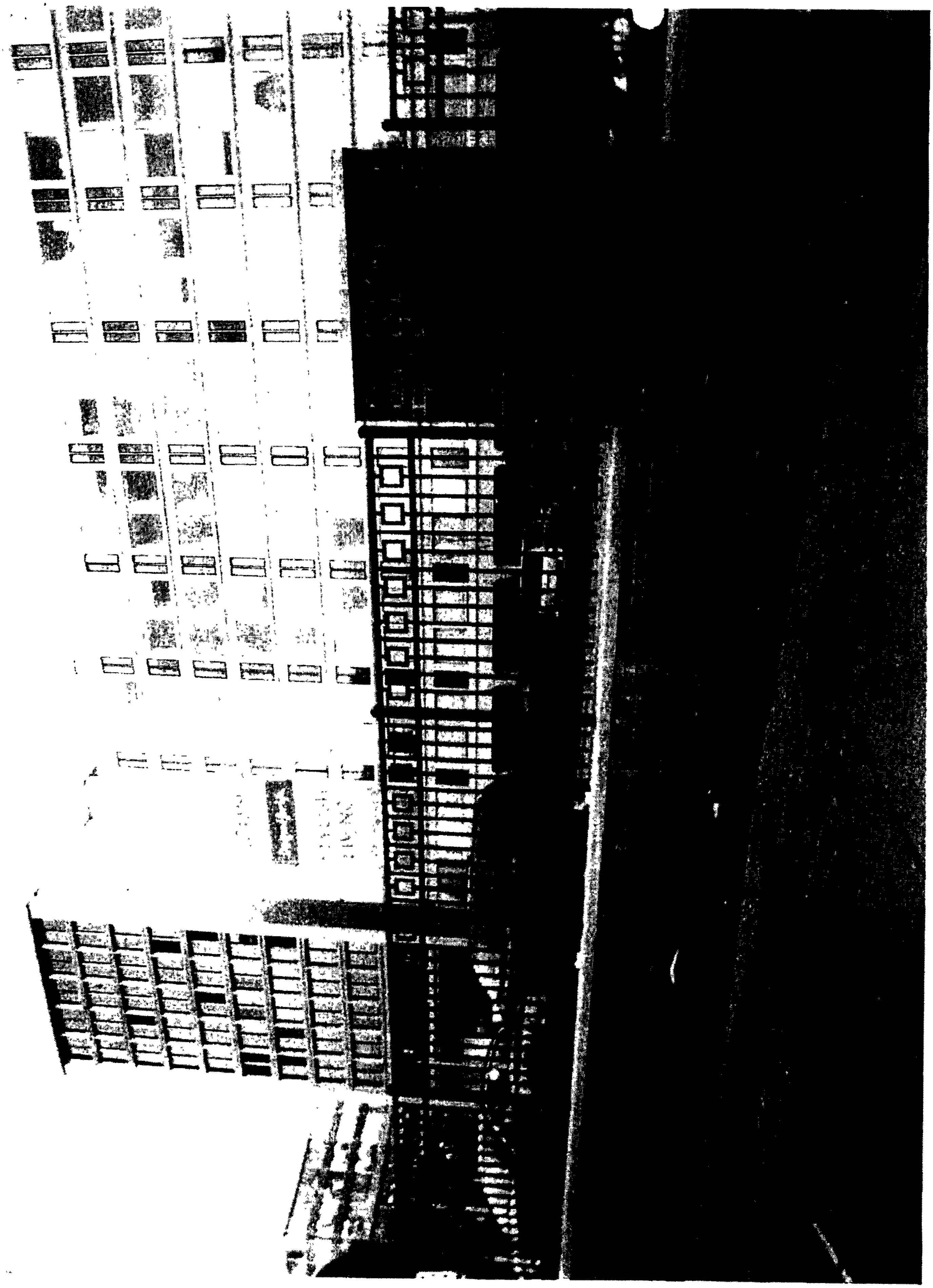
11-037-M-01

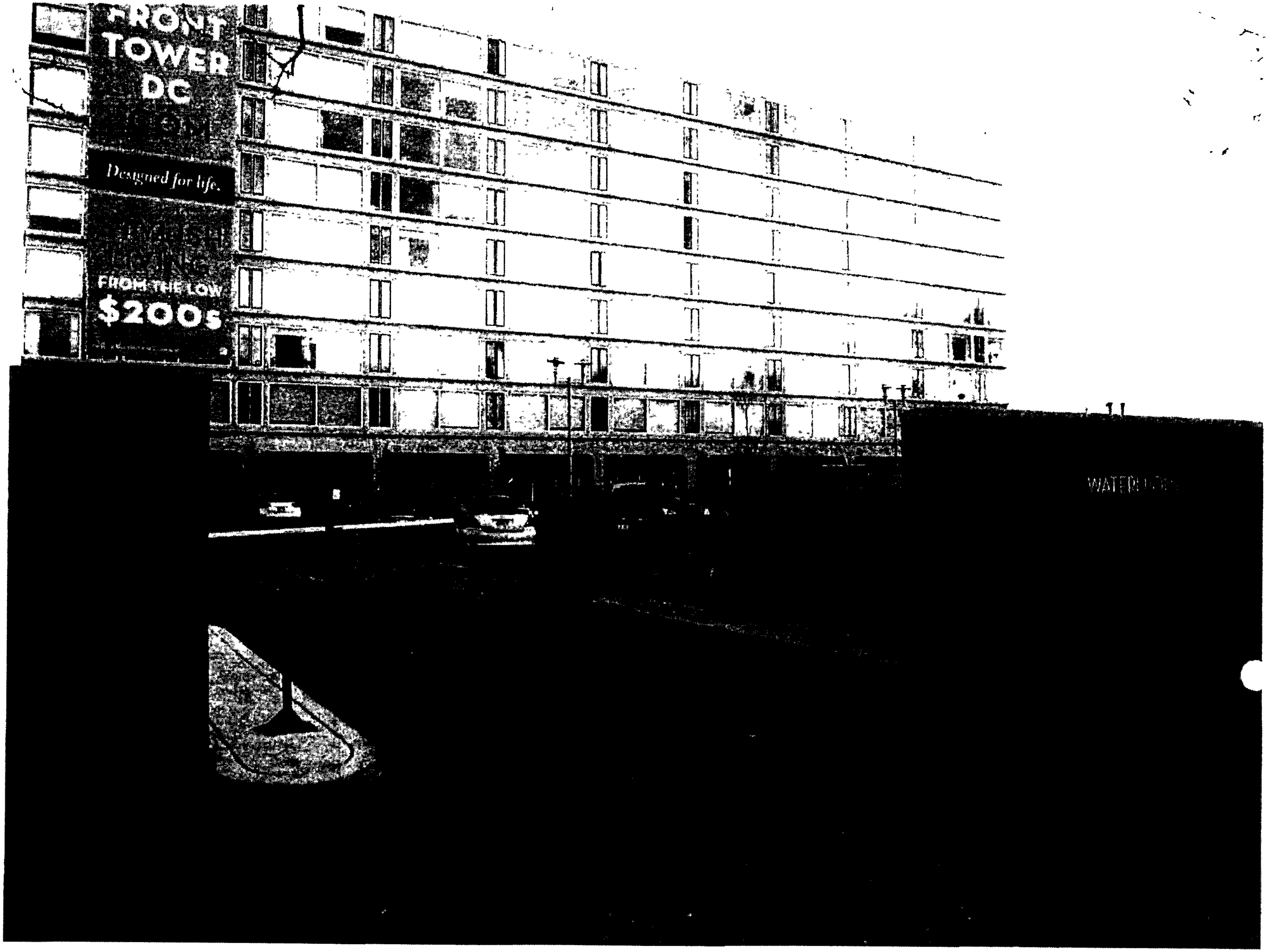
ATTACHMENT A
LOCATION TO BE SEARCHED

The SUBJECT PREMISES is located at 1101 3RD STREET SW, APARTMENT 304, WASHINGTON, DISTRICT of COLUMBIA 20024. The SUBJECT PREMISES is located on the corner of M Street SW and 3rd Street SW. The SUBJECT PREMISES is a high-rise, multi-family, apartment building, also known as the "Waterfront Tower" building. The number 1101 is located on the right pillar directly in front of the main entrance into the Waterfront Tower building. The Waterfront Tower is a gated community with electronic keypad access into the parking lot, the main building entrance, and into the exterior stairwells and interior elevators. The entrance into the building parking lot was located off of M Street near the intersection of M Street SW and 3re Street SW. Apartment 304 is an interior unit and is located on the west side of the third floor of the main entrance building. Apartment 304 has a brown door with the numbers "304" located to the right side of the door.

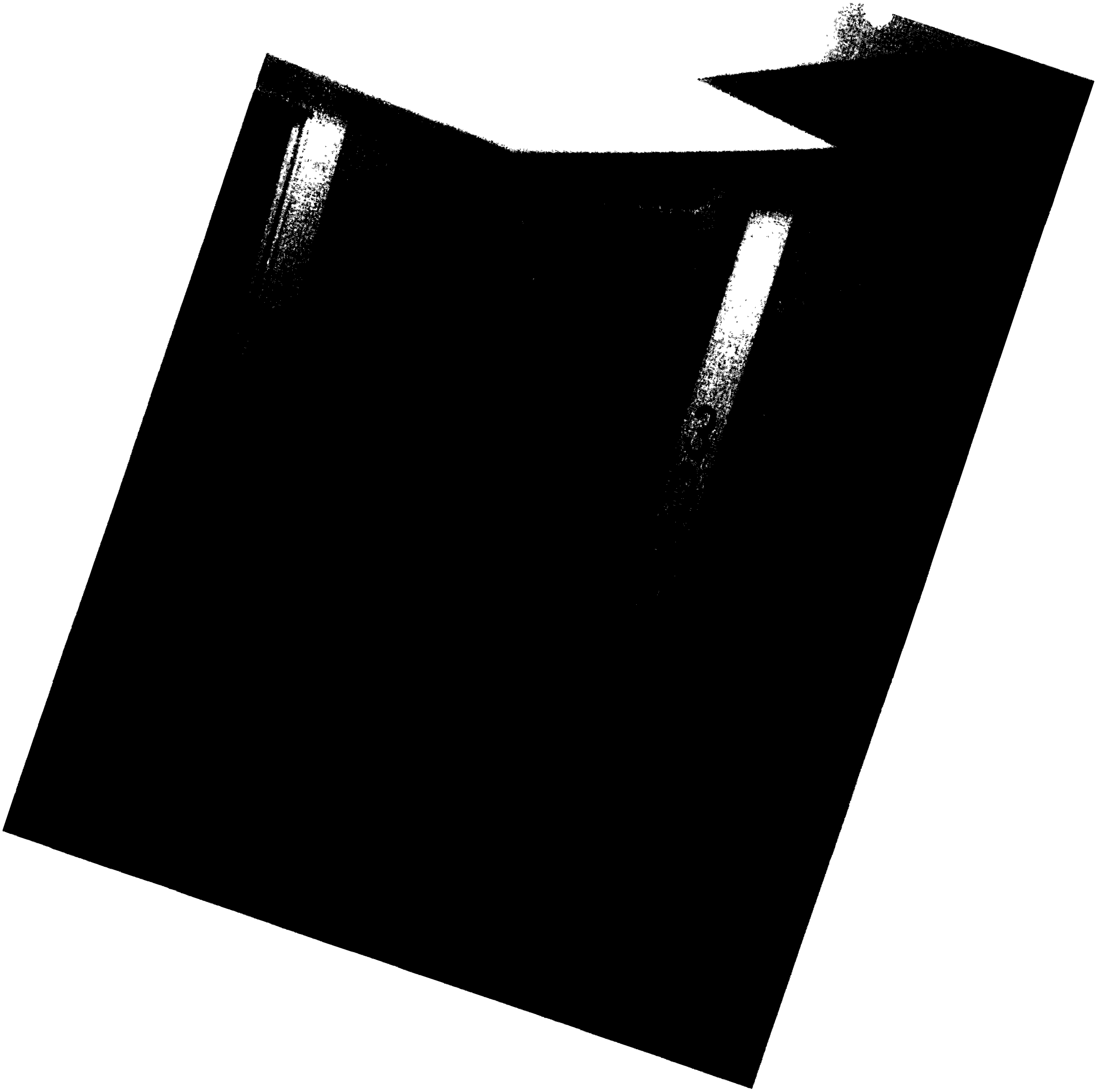
SUBJECT PREMISES PHOTOGRAPHS

(See Attachments)





FRONT TOWER DC
Designed for life.
FROM THE LOW
$200s
WATERI



11-037-M-01

ATTACHMENT B
ITEMS TO BE SEIZED

1. All records relating to violations of the statutes listed on the warrant since December 6, 2010, including:

a. Any digital device and/or computer capable of being used to commit, further commit or store evidence of the offense listed on the warrant.

b. Any equipment used to facilitate the transmission, creation, display, encoding or storage of digital data, including word processing equipment, modems, routers, and encryption devices;

c. Any magnetic, electronic, or optical storage devices capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMS, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, and personal digital assistants;

d. Any and all records, documents, and materials that relate to malicious software, code, or other programs associated with Trojans, botnets, denial of service attacks, to include but not limited to LOIC and/or HOIC;

e. Any and all records, documents, and materials that relate to communications between the seized computer hard drive and other computers involved in the denial of service attack, as well as to any individuals that may be controlling the denial of service attack or participating in the attack, to include IRC chat logs, other online chat logs, personal messages, twitter tweets, and/or email related to the denial of service attacks;

f. Any and all records, documents, and materials that relate to the administration, maintenance, operation, use or propagation of the denial of service tools, to include but not limited to LOIC/HOIC;

g. Any and all records, documents, and materials that relate to the identification and locations of person(s) using or controlling or disseminating denial of service software;

h. Any and all records, documents, and materials that relate to the identification and location of other computers comprising part of the denial of service attack and/or botnet;

i. Any and all data gathered or collected by means of the operation of the denial of service attack and/or botnet;

j. Any logs and other transactional information, to include but not limited to internet history, maintained in relation to computer(s) at the SUBJECT PREMISES;

k. Any and all records, documents, and materials that relate to the names, handles, email accounts or IP addresses of those at the SUBJECT PREMISES or those participants in the denial of service attack;

l. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software used in the digital device;

m. Any application, utility programs, compilers, interpreters and other software used to facilitate direct or indirect communication with the digital device;

n. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

o. Any passwords, password files, test key, encryption codes or other information necessary to access the digital device or data stored on the digital device.

2. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

3. Records and things evidencing the use of the Internet Protocol address 68.48.89.210 to communicate with PayPal's computer systems, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).